REMARKS/ARGUMENTS

The following Remarks accompany the Voluntary Amendment and Request for Continued Examination being submitted herewith with respect to the Examiner's final Office Action of February 7, 2006 to which the Applicant submitted a Reply on March 7, 2006.

Regarding Amendment

In the Amendment:

independent claims 1 and 6 are amended to recite that the first and second keys are secret keys, with subsequent cancellation of pending claims 2 and 7;

independent claim 1 is further amended to clarify that the claimed validation protocol is performed in a system, that the trusted and untrusted authentication chips are in communication with the system, and that the claimed comparison is performed using the system. Support for this amendment can be found, for example, at page 36, lines 1-13 of the present specification;

dependent claim 9 is amended to conform with amended claim 6; and

dependent claims 3-5, 8 and 10-12 are unchanged.

It is respectfully submitted that the above amendments do not add new matter to the present application, nor any new issues to the prosecution of, the present application.

Regarding 35 USC 103(a) Rejections

It is respectfully submitted that the subject matter of amended independent claims 1 and 6, and dependent claims 3-5 and 8-12, is not taught of suggested by Shigenaga (US 4,710,613) in view of Lee (US 5,923,759) or further in view of Abraham et al. (US 4,799,061) or Thomlinson et al. (US 5,778,069), for at least the following reasons.

As was discussed in the Applicant's Replies to the previous and current final Office Actions, in the present invention (as is clearly recited in amended independent claims 1 and 6) a random number is generated in the trusted chip of the system, a keyed one way function is applied to the random number in the trusted chip using a first secret key to produce a first encrypted outcome and in the untrusted chip of the system using a second secret key to produce a second encrypted outcome, the encrypted outcomes are compared in the system without knowledge of the secret keys, and the comparison result is used to determine the validity of the untrusted chip.

In the Response to Arguments/Amendment section of the current final Office Action, the Examiner admits that Shigenaga merely discloses using RSA to encrypt a random number in the card terminal using public keys and decrypt the encryption result in the IC card using private keys, and then comparing the random number and decryption result using the card terminal to determine the validity of the IC card (see col. 5, line 23-col. 9, line 24 of Shigenaga).

Thus, the process disclosed by Shigenaga does not use private keys in both the card terminal and IC card nor does the process perform encryption using such private keys in both the card terminal and IC card, as is required by amended independent claims 1 and 6.

The Examiner attempts to make up for these deficiencies in Shigenaga by citing Lee. However, Lee merely discloses using either symmetric (e.g., ECB) or asymmetric (e.g., RSA) encryption to encrypt a random number in the card using an 'internal' key and decrypt the encryption result in the processor using an 'identifying' key OR to encrypt a random number in the processor using the 'identifying' key and decrypt the encryption result in the card using the 'internal' key, and comparing the random number and decryption result using the processor to determine the validity of the card (see col. 6, line 37-col. 7, line 16 of Lee).

Thus, the processes disclosed by Lee may use either public/private or private/private key pairs in the processor and card, but like Shigenaga, the processes do not perform encryption using private keys in both the processor and card, as is required by amended independent claims 1 and 6.

Whilst the Examiner appears to recognise these distinctions between the claimed invention and both Shigenaga and Lee, the Examiner asserts, in the Response to Arguments/Amendment section of the current final Office Action, that the disclosure in Lee of a process in which the card encrypts the random number would lead one of ordinary skill in the art to modify the process of Shigenaga in this way.

However, it is respectfully submitted that since both Shigenaga and Lee clearly only disclose processes in which encryption is performed by one of a 'trusted' chip and a 'untrusted' chip, decryption is performed by the other of the trusted and untrusted chips, and comparison of the original and decrypted random numbers is performed, then any combination of Shigenaga and Lee would include such a encryption/decryption process, in contrast to the encryption/encryption process if amended independent claims 1 and 6.

This is because, the disclosure of neither Shigenaga nor Lee would suggest to one of ordinary skill in the art to perform an encryption/encryption process in which separately encrypted random numbers are compared. Further, it is respectfully submitted that one of ordinary skill in the art would only arrive at such an encryption/encryption process from the disclosures of Shigenaga and Lee by using hindsight from the disclosure of the present application, which of course is impressible with respect to determining patentability.

Furthermore, it is respectfully submitted that since Shigenaga specifically teaches that RSA encryption is preferred (see col. 8, lines 53-58 of Shigenaga) and Lee teaches that RSA encryption is suitable, then in any combination of Shigenaga and Lee, RSA encryption would be used. Accordingly, two secret keys would not be used as required by amended independent claims 1 and 6.

As was discussed in the Applicant's Replies to the previous and current final Office Actions, neither Abraham nor Thomlinson make up for these deficiencies in Shigenaga and Lee either taken alone or in combination.

It is respectfully submitted that the present application is in condition for allowance and reconsideration of the present application is respectfully requested.

Very respectfully,

Applicants:

Simon Robert Walmsley

Paul Lapstun

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia
Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762